memoori

SMART BUILDINGS

Cybersecurity for Smart Commercial Buildings

The BIOT Creates New Cybersecurity Vulnerabilities

An estimated **2.7 BILLION DEVICES** are already connected in Smart Buildings[3]

140 (2011) 243 (2014)

US Cybersecurity breaches involving building control systems[4]

9% of Building Automation Systems were linked to known vulnerabilities in 2014[5]

IP Cameras linked to the Internet[5]

392,115 HIKVISION **392,817** DAHUA

84% Building Automation Systems with Internet connections[1]

75% Organizations without formal cybersecurity incident response[2]

29% Organisations that have taken action to improve cybersecurity[1]

BY 2018, 20% OF SMART BUILDINGS WILL HAVE SUFFERED some form of digital vandalism[7]

The Cybersecurity Life Cycle

1 RECONNAISSANCE & PLANNING
Identify and profile the target. Investigate potential means of entry to their systems.

2 WEAPONIZATION
With potential vulnerabilities established, build or acquire relevant tools to exploit the victims systems.

3 DELIVERY
Begin the attack campaign via weaponized assets to the victim via email, web, or USB, or social engineering attack.

4 EXPLOITATION & SPREAD
Exploit established vulnerabilities to execute code that established a foothold on the victim's system/networks.

5 C&C
Take over control of any compromised assets and develop outbound communication channels.

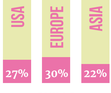
6 EXFILTRATION & IMPACTS
With access and control established, carry out harmful attacks or exfiltration of vulnerable data.

Multiple Potential Threat Actors

IMPACTS & CONSEQUENCES

CONFIDENTIAL DATA LOSS	IP LOSS, COMMERCIAL DATA LOSS, IDENTITY THEFT, POTENTIAL FOR FRAUD OR EXTORTION
BUILDING SYSTEMS DISRUPTION OR FAILURE	CAN RANGE FROM A NUISANCE TO A THREAT TO HUMAN LIFE. LOST PRODUCTIVITY, PHYSICAL SYSTEMS DAMAGE
BRAND AND REPUTATIONAL DAMAGE	LOSS OF CUSTOMER TRUST, DECREASED REVENUE, CUSTOMER CHURN
LEGISLATOR SCRUTINY	INVESTIGATIONS, FINES AND REMEDIATION

Drivers & Challenges



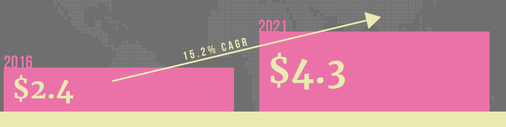
SKILLS
Percentage of companies unable to fill open cyber security positions in their enterprises[8]

CYBERSECURITY CONCERNS
Cybersecurity risks remain the leading cause for concern that is hindering the rollout of the IoT in multiple surveys

PREPAREDNESS
66 percent say this is the top barrier to cyber resilience.[2]

GLOBAL MARKET FOR CYBERSECURITY IN SMART COMMERCIAL BUILDINGS

($ Billion)



BEST PRACTICE FOR CYBER THREAT MITIGATION

- Perform risk assessments & security audits
- Develop and adopt safeguards, standards and corporate policies for cybersecurity across the organisation
- Build security awareness & collective responsibility across the organisation & your supply chain
- Adopt a layered security approach, with security embedded all the way from the device to the perimeter

memoori

SOURCES:
[1]IBM X-Force [2]Ponemon Institute [3]Memoori, The Market for IoT in Smart Commercial Buildings 2016
[4]US Government Accountability Office (GAO) [5]Malchow and Klick (2014) [6]Shodan.io [7]Gartner
[8]ISACA's State of Cyber Security 2017 [9]Cybersecurity Ventures